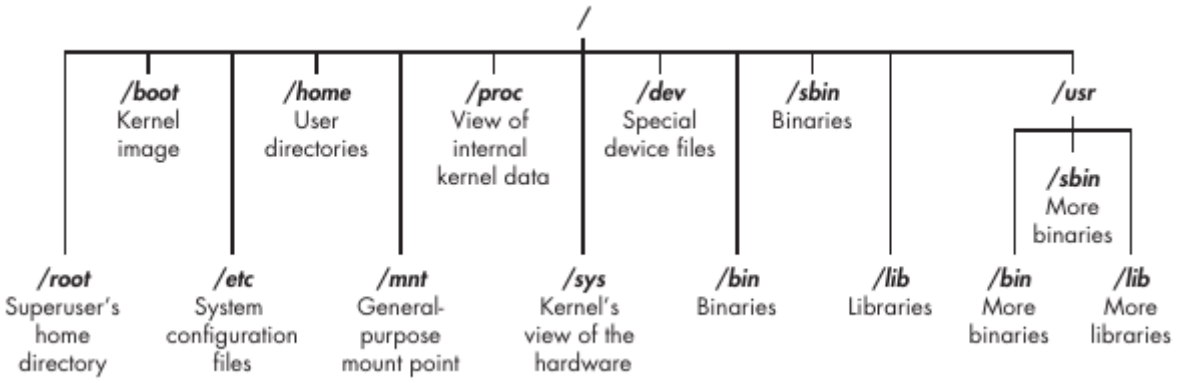
Drzewo katalogów



Korzeń (**/**) systemu plików znajduje się na szczycie drzewa, a najważniejsze podkatalogi, o których należy wiedzieć, to:

/root Katalog domowy wszechpotężnego użytkownika root
/ect Ogólnie zawiera pliki konfiguracyjne Linuksa, które kontrolują kiedy i jak uruchamiają się programy
/home Katalog domowy użytkownika
/mnt Gdzie inne systemy plików są dołączone lub zamontowane do systemu plików
/media Gdzie dyski CD i urządzenia USB są zwykle dołączane lub montowane w systemie plików
/bin Miejsce, w którym znajdują się pliki binarne aplikacji (odpowiednik plików wykonywalnych w systemie Microsoft Windows lub aplikacji w systemie macOS).
/lib Gdzie znajdziesz biblioteki (udostępnione programy podobne do bibliotek DLL systemu Windows)

kali >pwd → pokaż aktualne położenie
kali>whoami → jako kto jestem zalogowany
kali >cd /etc → “cd” - change directory → zmień katalog
kali:/etc/etc>pwd
kali:/etc >cd .. → przejdź katalog wyżej
kali >pwd
kali >cd /usr/share/fonts → “cd” - change directory → zmień katalog
kali >cd ../.. → przejdź o 2 katalogi wyżej
kali >ls -l → lista plików w formie “listy” → nazwa pliku, właściciel, uprawnienia, wielkość …
kali >ls -la → “a” → all → wszystkie pliki (też te ukryte z kropką na początku np. **.**bash_history)
kali >ls -h
kali >nmap -h → pomoc dla nmap
kali >aircrack-ng --help
kali >man ls → “man” manula - podręcznik
kali >locate aircrack-ng → lokalizacja plików
kali >updatedb → aktualizacja bazy plików locate
kali >whereis aircrack-ng → zwraca nie tylko lokację plików ale też stronę manula
kali >which aircrack-ng → zwraca lokalizację pliku jeśli jest ona ujęta w zmiennej $PATH
/usr/bin/aircrack-ng
kali >find / -type f -name apache2 → znajdź plik w lokacji / (główny katalog) , typ pliku (f - file), nazwa apache2
kali >find /etc -type f -name apache2.* → znajdzie plik /etc/apache2/apache2.conf
kali >ps aux → pokaż działające procesy (ax -aktywne procesy, u - wraz z użytkownikami)
kali > touch hackingskills
kali >echo ‘A white hat is an ethical security hacker.’ > hackingskills → (przekierownie potoku)
kali >echo ‘The white hat is contrasted with the black hat.’ >> → hackingskills (dopisywanie)
kali >cat hackingskills → odczytanie pliku
kali >cat >> hackingskills (tryb interaktywny możemy **dopisywać** dane → ctrl+D)

kali >cat > hackingskills (tryb interaktywny możemy **nadpisywać** dane → ctrl+D)
kali >mkdir newdirectory
kali >cd newdirectory
kali >touch oldfile
kali >cp oldfile /root/newdirectory/newfile
kali >cd newdirectory
kali >ls
kali >mv newfile newfile2
kali >ls
kali >rm newfile2
kali >rmdir newdirectory → błąd " Directory not empty"
kali >rm -r newdirectory → usuwanie rekurencyjne

Zadania:

1. Użyj polecenia ls z katalogu głównego (/), aby przejrzeć strukturę katalogów systemu Linux. Przejdź do każdego z katalogów za pomocą polecenia cd i uruchom pwd, aby sprawdzić, gdzie jesteś w strukturze katalogów.
2. Użyj polecenia whoami, aby zweryfikować, jako użytkownik jesteś zalogowany.
3. Użyj polecenia lokalizacji, aby znaleźć listy słów (wordlists), których można użyć jako hasła cracking.
4. Użyj polecenia cat, aby utworzyć nowy plik, a następnie dołącz do tego pliku.
Pamiętaj, że > przekierowuje dane wejściowe do pliku, a >> dołącza do pliku.
5. Utwórz nowy katalog o nazwie hackerdirectory i utwórz w nim nowy plik ten katalog o nazwie hackedfile. Teraz skopiuj ten plik do katalogu /root i zmień jego nazwę na secretfile.

Zarządzanie i manipulacja tekstem

kali >cat /etc/snort/snort.conf
(Snort – sieciowy system wykrywania i zapobiegania włamaniom (IPS). Może być również wykorzystywany jako sniffer (podobnie jak tcpdump) lub rejestrator pakietów)
kali >head /etc/snort/snort.conf (head ang. głowa - przeglądanie pliku od góry)
kali >tail -20 /etc/snort/snort.conf (tail ang. ogon - przeglądanie pliku od dołu)
kali >nl /etc/snort/snort.conf (number lines)
kali >cat /etc/snort/snort.conf | grep output (grepowanie - filtrowanie w poszukiwaniu ciągów znaków)
kali >tail -n+507 /etc/snort/snort.conf | head -n 6 (przeglądanie pliku od 507 linii do 512)
kali >cat /etc/snort/snort.conf | grep mysql (pionowa linia oznacza przekierowanie potoku do innego programu)
kali >sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf *(zastęp.ciągów znaków sed (ang. stream editor) – edytor strum.)*
kali >cat snort2.conf | grep MySQL
kali >sed s/mysql/MySQL/ snort.conf > snort2.conf (zastępowanie tylko pierwszego - bez global "g")
kali >sed s/mysql/MySQL/2 snort.conf > snort2.conf (zastępowanie tylko drugiego wystąpienia)
kali >more /etc/snort/snort.conf
kali >less /etc/snort/snort.conf
kali >cat /etc/passwd | cut -d":" -f1 (wyświetlenie 1szej kolumny -f1 wydzielonej przez separator/delimiter w postaci dwukropka)
kali >cat /etc/passwd | cut -d":" -f1 | grep ^k[a-z]* (filtr w poszukiwaniu słów zaczynających się ^ od k i skład. się z liter)
kali >cat /etc/passwd | cut -d":" -f1 | grep ^k[a-z]*i$ (filtr w poszukiwaniu słów kończących $ się na literę i)

ZADANIA
1. Przejdź do „/usr/share/metasploit-framework/data/wordlists". To jest katalog wielu list słów, których można użyć do brutalnego użycia haseł w różnych urządzeniach chronionych hasłem za pomocą Metasploit, najpopularniejszego frameworka do pentestu i hakowania.
2. Użyj polecenia cat, aby wyświetlić zawartość pliku „password.lst".
3. Użyj polecenia more, aby wyświetlić plik „password.lst".
4. Użyj polecenia less, aby wyświetlić plik „password.lst".
5. Teraz użyj polecenia nl, aby umieścić numery linii na hasłach w "password.lst". Powinno być około 88 396 haseł.

6. Użyj polecenia „tail”, aby wyświetlić ostatnie 20 haseł w pliku password.lst.
7. Użyj polecenia „cat”, aby wyświetlić plik „password.lst” i potokuj go, aby znaleźć wszystkie pliki hasła zawierające 123.

Zarządzanie i przeglądanie sieci

kali >ifconfig
(1)eth0: flags=4163<UP, Broadcast, RUNNING, MULTICAST> mtu 1500
(2)inet addr:192.168.181.131 netmask 255.255.255.0
(3)Bcast:192.168.181.255
--snip--
(4)lo Linkencap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
--snip--
(5)wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02

(1) nazwa pierwszego interfejsu eth0, mtu Maximum transmission unit (MTU)
(2) adres sieciowy wraz z maską
(3) adres rozgłoszeniowy
(4) lo (loopback address - inna nazwa localhost [127.0.0.1]) interfejs wirtualny
(5) wlan0 - interfejs sieci bezprzewodowej

kali >iwconfig
wlan0 IEEE 802.11bg ESSID:off/any
Mode:Managed Access Point: Not Associated Tx-Power=20 dBm
--snip--
lo
no wireless extensions
eth0
no wireless extensions
Standard 802.11b pozwala osiągnąć zasięg ok. 47 m w pomieszczeniu oraz ok. 98 m na otwartej przestrzeni. Do 11 Mb/s
Standard 802.11g pracuje on podobnie jak 802.11b na częstotliwości 2,4 GHz, ale pozwala na transfer z prędkością 54 Mb/s.
Adapter wlan0 jest nie podłączony (Not Associated) do access pointa (AP) i jego moc wynosi 20 dBm

kali >ifconfig eth0 192.168.181.115
kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast 192.168.1.255
kali >ifconfig eth0 down *(wyłączenie interfejsu)*
kali >ifconfig eth0 hw ether 00:11:22:33:44:55 *(fałszowanie adresu MAC)*
kali >ifconfig eth0 up *(załączenie interfejsu)*
kali >dhclient eth0
kali >ifconfig
kali >dig hackers-arise.com ns
(badanie DNS z dig)
kali >dig hackers-arise.com mx

SEKCJA DODATKOWA - zapytanie dig ujawnia adres IP
adres (216.239.32.100) serwera DNS obsługującego hackers-arise.com. Można także użyć polecenia Dig, aby uzyskać informacje na e-mail
serwery podłączone do domeny, dodając opcję mx (mx to skrót od
mail exchange server). Te informacje są krytyczne dla ataków na systemy pocztowe

```
cyt@cytlap:~$ dig hackers-arise.com ns

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> hackers-arise.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27762
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;hackers-arise.com.             IN      NS

;; ANSWER SECTION:
hackers-arise.com.      86400   IN      NS      ns6.wixdns.net.
hackers-arise.com.      86400   IN      NS      ns7.wixdns.net.

;; ADDITIONAL SECTION:
ns7.wixdns.net.         82      IN      A       216.239.34.100
ns6.wixdns.net.         396     IN      A       216.239.32.100

;; Query time: 204 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Aug 03 09:38:52 CEST 2023
;; MSG SIZE  rcvd: 124
```

Polecenia obsługi systemu	
Podstawy terminala	
cd ~ mkdir ~/Dokumenty/Faktury cd ~/Dokumenty/Faktury touch faktura{1..31}styczen.pdf	
ls ls -l ls -lht ls > listaPlikow.txt ls ~/Dokumenty/Faktury > listaFaktur.txt less ~/Dokumenty/Faktury/ listaFaktur.txt	lista plików -l rozbudowana lista plików -t sortowanie wg czasu -h human readable (MB, GB) Utworzenie listy plików z aktualnego katalogu
pwd	obecna lokalizacja w formie ścieżki
cd nazwa_katalogu → cd ~/Pulpit cd ~ cd / cd .. cd ../../../	przejście do katalogu przejście do katalogu domowego przejście do katalogu główny (root) przejście katalog wyżej przejście 3 katalogi wyżej
cp cp źródło miejsce_docelowe cp ~/Pulpit/ulubione_filmy.odt ../ cp -r ~/Pulpit ~/Kopia_Pulpitu	kopiowanie pliku skopiowanie pliku ulubione_filmy.odt z katalogu domowego katalog wyżej kopiowanie z podkatalogami
mv mv ~/Pulpit/ulubione_filmy.odt ~/Dokumenty mv ~/Pulpit/ulubione_filmy.odt ~/Pulpit/ulubione.odt	przesuwanie lub zmiana nazwy przeniesienie pliku z pulpitu do dokumentów Zmiana nazwy
rm plik rm ~/Pulpit/ulubione.odt rm -r ~/Domumenty/faktury	usuwanie pliku usunięcie pliku ulubione.odt usunięcie katalogu z podkatalogami (-r rekursywnie)
mkdir mkdir ~/Pulpit/Muzyka mkdir -p ~/Pulpit/dokumenty/faktury/2021	tworzenie katalogu utworzenie katalogu Muzyka na pulpicie utworzenie katalogu z podkatalogami

touch touch ~/Pulpit/test touch plik0{1..9}.txt	tworzenie pliku tekstowego utworzenie pliku test tworzenie wielu plików z licznikiem
grep grep Wzór Plik grep -i do litwo.txt ps ax | grep mc less /var/log/auth.log | grep failure	grep szukanie wzorca w pliku tekstowym szukamy frazy “do” w pliku litwo.txt z ignorowaniem wielkości znaków wyszukiwanie procesu po nazwie Pokazuje błędne logowania do systemu Filtruje plik auth.log w poszukiwaniu frazy “failure”
df -h /home	Pokaż wolne miejsce na partycji, -h → MB, GB, kB
du -sh /home	Pokaż ile zajmuje dany katalog -s suma -h → MB, GB, kB
wget https://wolnelektury.pl/media/book/txt/pan-tadeusz.txt wget ftp://192.168.18.100/pub/pan-tadeusz.txt cat pan-tadeusz.txt cat pan-tadeusz.txt pan-tadeusz.txt pan-tadeusz.txt > litwy.txt	wyświetl plik i wyjdź łączenie plików
more pan-tadeusz.txt less litwy.txt	proste przeglądarki plików tekstowych
tail -20 /var/log/auth.log	przeczytaj ostatnich 20 linijek
head -20 /var/log/auth.log	przeczytaj pierwszych 20 linijek
diff litwo.txt litwo1.txt	sprawdza różnice między plikami
ln -s CEL NAZWA_DOWIĄZANIA ln -s /etc ~/skrot_etc ln -s ~/Dokumenty ~/Pulpit/dokumenty	Tworzy skrót do pliku lub katalogu Tworzy skrót skrót_etc w kat.dom. Tworzy skrót dokumenty na Pulpicie ls -l lrwxrwxrwx … /etc → ~/skrot_etc
ps ax	wyświetlanie procesów
kill 2345	likwidacja procesu o pid 2345
systemctl status usługa systemctl status apache2 systemctl status ssh sudo systemctl start ssh sudo systemctl stop ssh	Status usługi systemowej (active, inactive) Status apache i ssh Uruchomienie Zatrzymanie

chmod 700 litwo.txt 1 → x execute 2 → w write 4 → r odczyt 7=4+2+1 (rwx) 6=4+2 (rw) 3=2+1 (xw) chmod u+r litwo.txt chmod u+rx litwo.txt chmod g+r litwo.txt chmod o+rwx litwo.txt chmod a-rw litwo.txt	zmiana uprawnień dla pliku litwo.txt (właściciel ma pełne uprawnienia, pozostali nic) dodanie uprawnień odczytu dla właściciela u - user - właściciel g - group - grupa o - others - pozostali a - all - wszyscy u+r → nadanie praw odczytu dla właściciela u+rx → dodanie odczytu i wykonania g+r → dodanie grupie praw odczytu o+rwx → nadanie pozostałym wszystkich praw a-rwx - zabranie wszystkim wszystkich praw (odczyt,zapis,wykonanie)
less /etc/passwd	pokazuje wszystkich użytkowników
less /etc/group	pokazuje wszystkie grupy
chown sudo chown root litwo.txt sudo chown root:users litwo.txt	zmiana właściciela zmiana właściciela
sudo chgrp grupa plik.txt	zmiana grupy dla pliku
sudo useradd -m -G users -s /bin/bash adminzsp	Tworzymy użytkownika z katalogiem domowym (-m) w grupie users (-G users) z dostępem do shella (-s /bin/bash). adminzsp → nazwa użytkownika
sudo chown news:www-data /var/log/syslog	zmiana właściciela na news i grupy na www-data dla pliku syslog
sudo userdel -r adminzsp	usuwanie użytkownika z katalogiem domowym
sudo usermod -a -G sudo,users,root adminzsp	Modyfikacja użytkownika -a (add dodaj do grupy …)
sudo groupadd nazwagrupy sudo groupdel nazwagrupy sudo groupmod staragrupa -n nowagrupa	dodawanie grupy usuwanie grupy zmiana nazwy grupy

gpasswd --delete uzytkownik grupa	usuwanie użytkownika z 1 grupy
echo użytkownik:hasło | sudo chpasswd	Zmiana hasła w sposób jawny (wykorzystywane w skrypcie bash)
mkdir zasoby cd zasoby touch user.sh chmod +x user.sh nano user.sh *!#/bin/bash* *echo tester:T@jneHaslo# | sudo chpasswd* **Zapisujemy przez ctrl+x i Y/T** ./user.sh	TWORZENIE SKRYPTU **ZMIENIAJĄCEGO HASŁO** UŻYTKOWNIKOWI tester tworzenie katalogu zasoby przejście do katalogu tworzenie pustego pliku user.sh dodanie praw wykonania (eXec) edycja pliku skryptu user.sh Dodanie interpretera bash wyświetlanie tekstu tester:T@jneHaslo# i przekierowanie go do polecenie chpasswd uruchomienie skryptu. Plik jest w tym samym katalogu gdzie się znajdujemy więc używamy: **./**nazwa_skryptu.sh
mkdir zasoby cd zasoby touch user.sh chmod +x user.sh nano user.sh *!#/bin/bash* *sudo useradd -m -s /bin/bash student* *echo student:T@jneHaslo# | sudo chpasswd* **Zapisujemy przez ctrl+x i Y/T** ./user.sh	TWORZENIE SKRYPTU **DODAJĄCEGO** UŻYTKOWNIKA student tworzenie katalogu zasoby przejście do katalogu tworzenie pustego pliku user.sh dodanie praw wykonania (eXec) edycja pliku skryptu user.sh Dodanie interpretera bash utworzenie użytkownika student z prawami do basha (-s shell) wyświetlanie tekstu tester:T@jneHaslo# i przekierowanie go do polecenie chpasswd uruchomienie skryptu. Plik jest w tym samym katalogu gdzie się znajdujemy więc używamy: **./**nazwa_skryptu.sh

Komendy do sprawdzania sprzętu	
lspci, lspci -vv	informacje nt. karty graficznej, dźwiękowej, sieciowej
lshw (list of hardware), lshw -short	CPU,GPU,MEM,NET
lscpu	informacje nt. CPU (nazwa, ile rdzeni CORE, ile wątków THREAD, częstotliwość FREQ MIN, MAX, ile pamięci podręcznej L1,L2,L3 (Level 1 …)
lsusb	wyświetla informacje nt. podłączonego sprzętu do portu USB
sudo dmidecode | more	informacje nt. BIOS, Płyty głównej, RAM ...
inxi -Fx	zbiór informacji o sprzęcie (instalujemy przez sudo apt install inxi)
sudo fdisk -l	Informacje o HDD